

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY


(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

REC'D 13 FEB 2006

WIPO

PCT

Applicant's or agent's file reference P18484-TPF	FOR FURTHER ACTION See Form PCT/PEA416	
International application No. PCT/EP 03/12141	International filing date (day/month/year) 31.10.2003	Priority date (day/month/year) 31.10.2003
International Patent Classification (IPC) or national classification and IPC G06F1/00		
Applicant TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) et al.		
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 8 sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input checked="" type="checkbox"/> sent to the applicant and to the International Bureau a total of 9 sheets, as follows:</p> <p><input type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</p>		
<p>4. This report contains indications relating to the following items:</p> <p><input checked="" type="checkbox"/> Box No. I Basis of the opinion</p> <p><input type="checkbox"/> Box No. II Priority</p> <p><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p><input type="checkbox"/> Box No. IV Lack of unity of invention</p> <p><input checked="" type="checkbox"/> Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p><input type="checkbox"/> Box No. VI Certain documents cited</p> <p><input type="checkbox"/> Box No. VII Certain defects in the international application</p> <p><input type="checkbox"/> Box No. VIII Certain observations on the international application</p>		
Date of submission of the demand 24.05.2005	Date of completion of this report 10.02.2006	
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Kerschbaumer, J Telephone No. +49 89 2399-2999	



**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP 03/12141

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.
- ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
- ☐ international search (under Rules 12.3 and 23.1(b))
 - ☐ publication of the international application (under Rule 12.4)
 - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)
2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):*

Description, Pages

1-41 as originally filed

Claims, Numbers

1-28 filed with telefax on 02.01.2006

Drawings, Sheets

1/5-5/5 as originally filed

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:
- ☐ the description, pages
 - ☐ the claims, Nos.
 - ☐ the drawings, sheets/figs
 - ☐ the sequence listing (*specify*):
 - ☐ any table(s) related to sequence listing (*specify*):
4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
- ☐ the description, pages
 - ☐ the claims, Nos.
 - ☐ the drawings, sheets/figs
 - ☐ the sequence listing (*specify*):
 - ☐ any table(s) related to sequence listing (*specify*):

* If item 4 applies, some or all of these sheets may be marked "superseded."

**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP 03/12141

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-28
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	1-28
Industrial applicability (IA)	Yes: Claims	1-28
	No: Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The following document is referred to in this communication:

D1: US-A-5 917 912 (GINTER KARL L ET AL) 29 June 1999 (1999-06-29)

D2: WO-00/20950 (Glassbrook, 13.04.2000)

The document D2 was not cited in the international search report. A copy of the document is appended hereto.

2 The present application does not meet the requirements of Article 33(3) PCT, because the subject-matter of independent claim 1 does not involve an inventive step.

2.1 Document D1 is regarded as being the closest prior art source to the subject-matter of claim 1.

Claim 1	Document D1
Method for control of usage of content, wherein protected content exists being usage restricted by one or more first usage rights specifying one or more usage restrictions and/or one or more usage permissions of the protected content at a user device (DI), the method comprising the steps of	"VDE content creator / Rules & control" Fig. 2 "This reflective distributed processing mechanism permits ROS 602 to securely distribute rights and permissions in a controlled manner, and effectively restrict the characteristics of use of information content." col. 76, lines 28-31

**INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(SEPARATE SHEET)**

International application No.

PCT/EP 03/12141

obtaining the content at the user device (DI) from the protected content in accordance with the one or more first usage rights by decrypting the protected content by a first content encryption key in a first secure environment (SEI) of the user device (DI) and by accessing the decrypted content in the first secure environment (SEI),	"a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting ,..." col. 9 lines 20-24
defining at least one usage right at the user device (DI), the at least one defined usage right specifying one or more usage restrictions and/or one or more usage permissions of the content at a recipient device (D2)	Fig. 2 and col. 76, lines 28-31
and the at least one defined usage right comprising a temporal restriction,	<p>"an expiration date/time field 986 specifying the expiration date and/or time for the rights record a right ID field 988 identifying a right" col. 152 lines 52-54</p> <p>"Other techniques for time aging may also be used, including for example techniques that use only user or site information, absolute points in time, and/or duration of time related to a subset of activities related to using or decrypting VDE secured content or the use of the VDE system" col. 129 lines 20-25</p>
verifying that the at least one defined usage right is a subset of the one or more first usage rights,	"allows user to customize their access rights by selecting a subset of rights authorized by a corresponding PERC" col. 156 lines 23-24

**INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(SEPARATE SHEET)**

International application No.

PCT/EP 03/12141

generating at the user device (DI) integrity protection information for the at least one defined usage right,	<p>"limits as specified by a PERC (permissions record) ... The resulting PERCs and/or URTs may be signed (e.g., using digital signatures)..." col. 246 lines 13-19</p> <p>"Seals may be employed as check values in database records (e.g., in PERC 808) and similar applications." col. 215 lines 60-62</p> <p>Remarks: a signature is an integrity protection of the PERCs (rights).</p>
encrypting the content with a content encryption key,	<p>"... distributed content (to, for many content applications, employ one or more content encryption keys that are unique to the specific VDE installation and/or user), private key techniques such as triple DES to encrypt content,..." col. 21 line 62 to col. 22 line 12</p>
encrypting the content encryption key with a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2),	<p>"Alternately, the key blocks 810 can be encrypted with the end user's public key" col. 128 lines 65-66 and Fig. 17</p>
communicating the encrypted content, the at least one defined usage right, the encrypted content encryption key, and the integrity protection information to the recipient device	<p>Fig. 2 and 86,</p> <p>"users may still be able to transfer some or all usage rights to another electronic appliance 600, " col. 332 lines 20-24</p>
restricting the one or more first usage rights in consequence of the definition and/or the communication of the at least one defined usage right to the recipient device (D2),	<p>Remark: "Transfer" implies that the originating device does not have the rights anymore, so the first rights are restricted. Otherwise it would be a copy.</p>

verifying at the recipient device (D2) the integrity of the at least one defined usage right based on the integrity protection information	"PERCs may be signed" col. 246 lines 13-19 Remark: A signature is intended to be checked, otherwise it would make no sense adding a signature.
decrypting at the recipient device (D2) the encrypted content encryption key with a decryption key corresponding to the key encryption key,	Fig. 66 and 67
decrypting the encrypted content with the content encryption key in a secure environment (SE2) of the recipient device	Fig. 66 and 67
applying the at least one defined usage right to the content in the secure environment (SE2), and using the content at the recipient device (D2) according to the applied at least one usage right,	"Even if a consumer has a copy of a video program, she cannot watch or copy the program unless she has "rules and controls" that authorize use of the program. She can use the program only as permitted by the "rules and controls." col. 53 lines 60-63

- 2.2 The subject-matter of claim 1 therefore differs from this known digital document system of D1 in that it abolishes the restriction of the one or more first usage rights when the temporal restriction expires.
- 2.3 The problem to be solved by this feature may therefore be regarded as how to re-enable the use of the content for device 1 after the content is no longer lent to device 2.
- 2.4 This problem is not considered to represent a technical problem, because the procedure of lending something to someone is clearly business related. The person skilled in the art would just be confronted with the problem and asked to modify the system of D1 to enable this business requirements, therefore not involving any

inventive activity.

- 2.5 In the case that someone would consider this business related requirements as inventive, D2 describes on page 12 line 29 to page 13 line 4:

"If the permission is lent or leased, the procedure also specifies that the secret key is associated with matching expiration times 102S and 102R (e. g., each corresponding to a twoweek period) at the sender and recipient computers, respectively, so that the secret key cannot be used (and therefore the data item cannot be used) at the sender computer until expiration time 102S is reached, and can be used at the recipient computer only until expiration time 102R is reached. In this way, the permission is effectively returned to the sender computer from the recipient computer when the expiration time is reached"

- 2.6 Consequently, the skilled person would arrive at all features of claim 1 without any inventive activity.

- 3 The independent claims 10, 20, 25 and 27 define the program and device corresponding to the method of claim 1. Therefore the same objection as above applies correspondingly to these claims.

- 4 The additional features of the dependent claims appear to be either known from D1 and D2 or usually applied methods in the field of DRM and, consequently, do not lead to an inventive subject matter (Article 33 PCT).

Claims

1. Method for control of usage of content, wherein protected content exists
being usage restricted by one or more first usage rights specifying one or
5 more usage restrictions and/or one or more usage permissions of the
protected content at a user device (D1), the method comprising the steps
of
- obtaining the content at the user device (D1) from the
protected content in accordance with the one or more first
10 usage rights by decrypting the protected content by a first
content encryption key in a first secure environment (SE1) of
the user device (D1) and by accessing the decrypted content in
the first secure environment (SE1),
 - defining at least one usage right at the user device (D1), the at
15 least one defined usage right specifying one or more usage
restrictions and/or one or more usage permissions of the
content at a recipient device (D2) and the at least one defined
usage right comprising a temporal restriction,
 - verifying that the at least one defined usage right is a subset of
20 the one or more first usage rights,
 - generating at the user device (D1) integrity protection
information for the at least one defined usage right,
 - encrypting the content with a content encryption key,
 - encrypting the content encryption key with a key encryption
25 key associated with the recipient device (D2) and/or an
operator of the recipient device (D2),
 - communicating the encrypted content, the at least one defined
usage right, the encrypted content encryption key, and the
integrity protection information to the recipient device (D2),
 - 30 - restricting the one or more first usage rights in consequence of
the definition and/or the communication of the at least one
defined usage right to the recipient device (D2),

AMENDED SHEET

- 5
- verifying at the recipient device (D2) the integrity of the at least one defined usage right based on the integrity protection information,
 - decrypting at the recipient device (D2) the encrypted content encryption key with a decryption key corresponding to the key encryption key,
 - decrypting the encrypted content with the content encryption key in a secure environment (SE2) of the recipient device (D2),
 - applying the at least one defined usage right to the content in
 - 10 the secure environment (SE2), and
 - using the content at the recipient device (D2) according to the applied at least one usage right,
 - abolishing the restriction of the one or more first usage rights when the temporal restriction expires.

15

2. The method according to claim 1, the method further comprising the steps of

- restricting or blocking or deleting the at least one defined usage right at the recipient device (D2) before the expiry of the
- 20 temporal restriction,
- communicating an indication of the restricting or blocking or deleting to the user device (D1).

3. The method according to claim 2, further comprising the step of

25 generating by the recipient device (D2) at least one received usage right that is a subset of the at least one defined usage right for the indication.

4. The method according to claim 3, further comprising the steps of

- applying the at least one received usage right at the user
- 30 device (D1) until the expiry of the temporal restriction.

5. The method according to claim 3, further comprising the steps of

AMENDED SHEET

- 5
- recognizing by the user device (D1) that the at least one received usage right relates to the at least one defined usage right and
 - using the content at the user device (D1) according to the at least one first usage right even within the time upon the expiration of the temporal restriction.

10 6. The method according to any of the preceding claims, wherein the step of communicating the at least one defined usage right to the recipient device (D2) is executed by

- 15
- communicating the at least one defined usage right from the user device (D1) to a rights server (DS),
 - associating by the rights server (DS) the at least one defined usage right with authorization information indicating a rights issuer authorization for the at least one defined usage right to the recipient device (D2),
 - communicating the at least one defined usage right and the authorization information from the rights server (DS) to the recipient device (D2),

20 and the recipient device (D2) verifies the rights issuer authorization based on the received authorization information.

25 7. The method according to any of the preceding claims further comprising the step of communicating to a charging server an indication about the communication of the at least one defined usage right.

30 8. The method according to any of the preceding claim, wherein an input unit of the user device (D1) receives at least one instruction from a user for defining the at least one usage right.

9. The method according to any of the preceding claims further comprising the step of defining at least one further usage right for at least one further

AMENDED SHEET

recipient device for controlling the usage of the content at the at least one further device.

10. A user device (D1) for controlling a usage of content at a recipient device
 5 (D2), the user device (D1) comprising at least a transmission unit and a processing unit, wherein protected content exists being usage restricted by one or more first usage rights specifying one or more usage restrictions and/or one or more usage permissions of the protected content at the user device (D1), and the processing unit is adapted to
 10 obtain the content from the protected content in accordance with the one or more first usage rights by decrypting the protected content with a first content encryption key in a first secure environment (SE1) of the user device (D1) and by accessing the decrypted content in the first secure environment (SE1), to define at least one usage right specifying one or
 15 more usage restrictions and/or one or more usage permissions of the content at the recipient device (D2), the at least one defined usage right comprising a temporal restriction, to verify that the at least one defined usage right is a subset of the one or more first usage rights, to generate integrity protection information for the at least one defined usage right, to
 20 encrypt the content with a content encryption key, to encrypt the content encryption key with a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2), the transmission unit is adapted to send the encrypted content, the at least one defined usage right, the encrypted content encryption key, and the
 25 integrity protection information to the recipient device (D2), the processing unit is adapted to restrict the one or more first usage rights in consequence of the definition and/or the communication of the at least one defined usage right to the recipient device (D2) and to abolish the restriction of the one or more first usage rights the when temporal
 30 restriction expires.

AMENDED SHEET

5

11. The user device according to claim 9, wherein the user device is adapted to load the protected content via a receiving unit and to store the protected content at a storage and/or to store pre-installed protected content at the storage.

10

12. The user device according to claim 9 or 10, further comprising a receiving unit and the receiving unit is adapted to receive an indication of a restricting or a blocking or a deleting of the at least one defined usage rights at the recipient device (D2) before the expiry of the temporal restriction.

15

13. The user device according to claim 12, wherein the indication comprises at least one received usage right that is a subset of the at least one defined usage right.

20

14. The user device according to claim 13, wherein the processing unit is adapted to apply the at least one received usage right until the expiry of the temporal restriction.

25

15. The user device according to claim 13, wherein the user device is adapted to recognize that the at least one received usage right relates to the at least one defined usage right and to use the content according to the at least one first usage right even within the time upon the expiration of the temporal restriction.

30

16. The user device according to any of the claims 9 to 13, wherein the processing unit is adapted to generate an instruction for a rights server (DS) to associate the at least one defined usage right with authorization information indicating a rights issuer authorization for the at least one defined usage right to the recipient device (D2) and to communicate the at least one defined usage right and the authorization information to the recipient device (D2), and the transmission unit is adapted send the

AMENDED SHEET

instruction and the at least one defined usage right to the rights server (DS).

5 17. The user device according to any the claims 9 to 14, wherein the transmission unit is adapted to send to a charging server an indication about the communication of the at least one defined usage right to the recipient device (D2).

10 18. The user device according to any of claims 9 to 15, the user device (D1) further comprising an input unit which is adapted to receive at least one instruction from a user and the processing unit is adapted to define the at least one usage right based on the at least one instruction from the user.

15 19. The user device according to any of the claims 9 to 16, wherein the processing unit is adapted to define at least one further usage right for at least one further recipient device for controlling the usage of the content at the at least one further recipient device.

20 20. A recipient device (D2) for a controlled usage of content, the recipient device (D2) comprising at least a receiving unit and processing unit, wherein the receiving unit is adapted to receive the content being encrypted by a content encryption key, at least one defined usage right specifying one or more usage restrictions and/or usage permissions of the content and the at least one defined usage right comprising a
25 temporal restriction, a content encryption key being encrypted by a key encryption key associated with the recipient device (D2) and/or an operator of the recipient device (D2), and integrity protection information for the at least one defined usage right, the processing unit is adapted to
30 verify the integrity of the at least one usage right based on the integrity protection information, to decrypt the encrypted content encryption key with a decryption key corresponding to the key encryption key, to decrypt the encrypted content with the content encryption key in a secure

AMENDED SHEET

environment (SE2), to apply the at least one defined usage right to the content in the secure environment (SE2), and to use the content according to the applied at least one defined usage right.

5 21. The recipient device according to claim 18, wherein the processing unit is adapted to generate an alert if the integrity of the at least one defined usage right is violated and to initiate an indication of the alert at an output unit.

10 22. The recipient device according to claim 18 or 19 further comprising a transmission unit and the processing unit is adapted to restrict or block or delete the at least one defined usage right before the temporal restriction expires and to generate an indication of the restricting or the blocking or the deleting, and the transmission unit is adapted to send the indication
15 to the user device (D1).

20 23. The recipient device according to claim 22, wherein the processing unit is adapted to generate at least one received usage right that is a subset of the at least one defined usage right for the indication.

24. The recipient device according to any of the claims 20 to 23, wherein the receiving unit is adapted to receive the at least one defined usage right and associated authorization information indicating a rights issuer authorization from a rights server (DS) and the processing unit is adapted
25 to verify the rights issuer authorization based on the received authorization information.

30 25. Computer program loadable into a processing unit of a user device (D1), the computer program comprising code adapted to execute a process for obtaining of content from protected content, the protected content being usage restricted by one or more first usage rights specifying one or more usage restrictions and/or one or more usage permissions of the protected

AMENDED SHEET

5 content at the user device (D1) wherein the content is obtained from the
protected content in accordance with the one or more first usage rights
by decrypting the protected content by a first content encryption key in a
first secure environment (SE1) of the user device (D1) and by accessing
the decrypted content in the first secure environment (SE1), to execute a
process for defining at least one usage right specifying one or more
usage restrictions and/or one or more usage permissions of the content
at a recipient device (D2) with the at least one defined usage right
comprising a temporal restriction, to execute a process for verifying that
10 the at least one defined usage right is a subset of the one or more first
usage rights, to execute a process for generating integrity protection
information for the at least one defined usage right, to execute a process
for encrypting the content with a content encryption key, to execute a
process for encrypting the content encryption key with a key encryption
15 key associated with the recipient device (D2) and/or an operator of the
recipient device (D2), and to initiate a process for a communication of the
encrypted content, the at least one defined usage right, the encrypted
content encryption key, and the integrity protection information to the
recipient device (D2), to execute a process for restricting the one or more
20 first usage rights in consequence of the definition and/or the
communication of the at least one defined usage right to the recipient
device (D2), and to execute a process for abolishing the restriction of the
one or more first usage rights when the temporal restriction expires.

25 26. The computer program according to claim 25, wherein the code is
adapted to execute steps of the method according to any of the claims 1
to 9 as far as related to the user device (D1).

30 27. A computer program loadable into a processing unit of a recipient device
(D2), the computer program comprising code adapted to execute a
process for a verification of the integrity of at least one defined usage
right based on integrity protection information for the at least one defined

AMENDED SHEET

- 5 usage right, the at least one defined usage right specifying one or more
usage restrictions and/or usage permissions for the usage of content and
the at least one defined usage right comprising a temporal restriction, to
execute with a decryption key a process for a decryption of an encrypted
content encryption key being encrypted by a key encryption key
associated with the recipient device (D2) and/or an operator of the
recipient device (D2), the decryption key corresponding to the key
encryption key, to execute in a secure environment with the content
encryption key a process for a decryption of the encrypted content being
10 encrypted with the content encryption key, to execute a process for
applying the at least one defined usage right to the content in the secure
environment (SE2) and to control a process for using the content
according to the applied at least one defined usage right.
- 15 28. The computer program according to claim 27, wherein the code is
adapted to execute steps of the method according to any of the claims 1
to 9 as far as related to the recipient device (D2).

AMENDED SHEET